Customer No. 24498
Attorney Docket No. RCA89462
Final Office Action Date: 3/16/2007

ᴚᴇᴄᴇıᴠᴇᴅ
CENTRAL FAX CENTER

MAR 2 2 2010

Remarks/Arguments

Claims 1-8, 10, 14, and 17-24 are pending.

Claim 1 has been amended to recite that the scrambled program is received from a service provider. Amended claim 1 is now consistent with the remaining independent claims in explicitly reciting that the scrambled program is received from a service provider that is a separate entity from the first device. Also, the examiner's statement that the first device can comprise either the server or the access device En-Seung as stated in the office action on page 7, lines 19-20 is obviated in view of the amendment as discussed further below.

Rejection of claims 1-5, 7, 8, 10, 14, 17 and 20-24 under 35 USC 103(a) in view of Tsuria and En-Seung.

For the reasons discussed previously, applicants submit that the subject claims are patently distinguishable over the teachings of Tsuria in view of En-Seung. Applicants further address below the examiner's additional comments set forth in the Final Rejection of March 16, 2007.

The comments below are provided with respect to claim 1, but are believed to apply to the remaining independent claims since these claims also recite features similar to those addressed with respect to claim 1.

At the outset, applicants again note that Examiner continues to misapply the teachings of Tsuria to the claimed invention. That is, the Examiner continues to allege that the second device recited in claim 1 corresponds to the VCR 130 of Tsuria. As discussed in great detail in applicants' previous responses and in the appeal brief, VCR 130 of Tsuria cannot correspond to the recited second device or presentation device because VCR 130 does not perform the steps of obtaining the descrambling key from the rebundled descrambling key or descrambling the scrambled data component using the descrambling key as recited in claim 1. As is amply clear from the teachings of Tsuria, VCR 130 functions as a **mechanism for storing data** provided from IRD 110. Nowhere does Tsuria disclose or suggest

that VCR 130 provides performs any of the functions associated with the second device, or the presentation device, recited in the current claims.

The Examiner ostensibly acknowledges the defect of the assertion that VCR 130 corresponds to the recited second device by citing the teachings of En-Seung. Specifically, the Examiner appears to suggest modifying VCR 120 of Tsuria to perform the encryption/decryption scheme of En-Seung in order to provide the limitations of claim elements (c), (d) and (e).

First we discuss why VCR 120 of Tsuria does not correspond to the recited second device, and then why even if the teachings of En-Seung is applied to VCR 120 the resulting arrangement fails to teach or suggest the recited second device.

Incidentally, applicants again note that the Examiner misapplies the teachings of Tsuria by stating that "Tsuria does not explicitly disclose receiving in said second device, said rebundled descrambling key." As previously discussed by applicants, Tsuria, for example, see figure 1, clearly shows that the data generated by IRD 110 is provided to VCR 130. The data is provided in the format of SDDS (scrambled digital datastream), see figure 2, which includes the ECM key replaced by the TECM key. Therefore, Tsuria clearly discloses VCR 130 receiving the SDDS bitstream, which includes a rebundled descrambling key.

In any event, the examiner now appears to be arguing that the IRD 110 and VCR 120 should be effectively considered to be a single device, wherein VCR 120 is modified by the teachings of En-Seung.

In the response to arguments, the Examiner states

> "in the encryption/decryption mechanism, the first device and the second device are functionally bundled together in order to encrypt/decrypt the digital content – i.e. both of them cannot be separated and functioned (sp) independently. Besides, the user is the customer for both the 1st device (e.g., IRD or set up box) as well as the 2nd device (e.g., presentation

*device) and therefore the user (customer) information or the user (customer)
key is indeed associated with both of the 1ˢᵗ device and the 2ⁿᵈ device in
view of the TECM key (i.e. transformed ECM key or re-bundled
descrambling key)."*

However, this argument is counter to the examiner's previous arguments
that IRD 110 corresponds to the recited first device and VCR 130 corresponds to
the recited second device. This argument also is not supported by the teachings
of Tsuria.

The present claims recite distinct first and second devices. There is no
disclosure or teaching in the present application that they are to be effectively
treated as a single device. Correspondingly, there is simply no teaching or
suggestion in Tsuria that the IRD and VCR are to be treated as a single device that
cannot be separated and function independently. The mere fact that one device
performs encryption and a second device performs decryption does not
necessarily lead to the conclusion that these devices now cannot be separated or
function independently.

As previously discussed, the goal of Tsuria is to provide a system for
recording digital data streams which, in addition to having other features,
overcome the problem of unusability of recordings after a change of removable
security elements (col. 2, lines 39-43). Tsuria addresses this goal by replacing an
ECM associated with a received program with a corresponding TECM. The TECM
is associated with the system of Fig. 1, and is not changed when the ECM key is
changed (col. 2, lines 44-64).

There is no basis in Tsuria for the assertion that the IRD 110 and VCR 130
cannot be separated and function independently. Tsuria refers to the TECM of
Fig. 1, but it is clear that the TECM is not associated with the VCR since the VCR
merely acts as a vehicle for storing the SDDS bitstream generated by IRD 110.
One would not similarly assert that display 100 cannot be separated and function

independently of IRD 110 merely because it receives the display signal from IRD 110 and is shown in Fig. 1.

Tsuria does disclose that the TECM is permanently associated with the system of Fig. 1, and mentions that the TECM may be particular to a user of the system and that the TECM may be stored in a combination of IRD 110 and smart card 120, but nowhere does Tsuria require that the TECM is also associated with VCR 120 or display 100, or that IRD 110 cannot be separate and functionally independent of VCR 120. In view of the above and the reasons discussed previously, applicants maintain that VCR 120 cannot correspond to the second device or presentation device as recited in the present claims.

We now address the suggested combination of VCR 120 with the encryption/decryption arrangement of En-Seung. As discussed below applicants submit that the additional teachings of En-Seung fail to overcome the defect of Tsuria.

As an initial matter, the server cannot correspond to the first device as alleged by the Office Action (page 7, lines 19-20) since the server does not receive the scrambled program from a service provider as recited by claim 1. In En-Seung, it is service server 12 that functions as the service provider. Since the service server 12 provides the scrambled program to terminal unit 10, and En-Seung does not disclose the service server 12 receiving the scrambled program from a service provider, service server cannot correspond to the recited first device. In the arrangement of En-Seung, it is the terminal unit 10 that must correspond to the recited first device.

Additionally, service server 12 encrypts the program using identity information associated with terminal unit 10. Thus, even if one could label service server 12 as the first device, such a designated first device still fails to rebundle a descrambling key using a unique key associated with the first device.

Furthermore, terminal unit 10 cannot correspond to the recited second device or presentation device because terminal unit 10 receives the scrambled program that is scrambled using a user key associated with terminal unit 10. That is, the program is scrambled with a key associated with itself rather than a different, first device, as required by claim 1. In fact, terminal unit 10 receives the scrambled program from a service provider, namely service server 12, not from a first device. Service server 12 receives the request from terminal unit 10 and provides the scrambled program with the necessary key information in response to the request (col. 6, lines 21-29).

Additionally, present claim 1 recites a rebundled descrambling key, which is uniquely associated with the first device. Even if terminal unit 10 could be construed to correspond to the recited second device or presentation device, En-Seung fails to overcome the defect of Tsuria because the encryption/decryption scheme used by En-Seung does not relate in any manner to a rebundled descrambling key as recited in the pending claims.

Rebundling of the descrambling key refers to a process comprising decrypting an encrypted descrambling key associated with the scrambling program and re-encrypting the descrambling key using a key associated with a first device to produce the rebundled descrambling key. Page 2, lines 24-28. Nowhere does En-Seung disclose or suggest in any way a system that generates or processes a rebundled descrambling key.

The Office action asserts that the descrambling key is "... considered as an 'encrypted content key' and the content key is considered as a temporary validation key that encrypts the digital content." Page 7, lines 10-12. A close examination of the teachings of En-Seung shows that the examiner has misinterpreted the teachings of En-Seung.

Applicant agrees that En-Seung teaches encrypting the digital content with the temporary validation key. However, the "encrypted content key" of En-Seung does not correspond to the recited rebundled descrambling key because there is

no decrypting of a key followed by a re-encryption of the decrypted key.
Rather, En-Seung teaches that service server 12 generates the key information
using identity characters transmitted by terminal unit 10, wherein the key
information is used to generate a user key, which is then used to generate the
temporary validation key, which is used to decrypt the content (col. 6, lines 59-63).
En-Seung describes a scheme having **layers of encryption**, that is, the key
information is used to generate a first key, which is then used to generate another
key that is used to decrypt the content, not a rebundling process wherein a
scrambled key is descrambled and then re-scrambled using another key. These
are entirely different operations and nowhere does En-Seung mention or suggest
the rebundling feature as recited in the present claims.

In view of the above, applicants submit that even if the teachings of Tsuria
and En-Seung are combined as suggested by the Office Action, the combined
arrangement still fails to teach the claimed invention because the combined
arrangement would produce a VCR 120 that receives encrypted program using a
key associated with the VCR, and uses an encryption scheme that uses a layered
approach rather than a rebundled descrambling key.

As to the statement regarding the use of a public/private key pair in Tsuria,
applicants are unclear as to the applicability of the assertion to the present claims.
Clearly in a public/private key pair arrangement different parts of the key pair can
be stored in different device, for example to provide authentication. However, the
fact that one part of the key is stored in one device and another part of the key is
stored in another device is unrelated to the fact that a first device rebundles a
descrambling key, and a second device receives and processes the rebundled
descrambling key as recited in claim 1. Thus, applicants submit that this assertion
is not germane to the present claims.

Finally, applicants are aware of the requirements of MPEP 2145 and submit
that this, and the previous, responses satisfy MPEP 2145. Applicants have
discussed the individual teachings of the cited references to show that neither
reference discloses or suggests each and every limitation of the pending claims,

Customer No. 24498
Attorney Docket No. RCA89462
Final Office Action Date: 3/16/2007

and therefore, even if the cited references are combined as suggested by the examiner, the combined references still lack each and every limitation of the pending claims. That is, the combined references still fail to disclose or suggest elements (c), (d), and (e) of claim 1 because none of the references disclose or suggest the recited second device. Tsuria fails to disclose or suggest that VCR 120 processes the rebundled descrambling key as required by the claims, and even if the VCR 120 can be modified in accordance with the encryption/decryption arrangement of En-Seung, the combination still fails to disclose or suggest every limitation of claim 1 because En-Seung does not disclose or suggest rebundled descrambling keys as recited. Therefore, it is believed that applicant has addressed the combination suggested by the examiner in a proper manner.

The independent claims recite features similar to those discussed above with respect to claim 1. In view of the above, applicants submit that the cited claims are patentably distinguishable over the suggested combination of Tsuria and En-Seung.

Rejection of claims 6 and 18 in view of Tsuria, En-Seung, and Wasilewski

Applicants submit that even assuming arguendo that Wasilewski provides the teachings alleged by the examiner, Wasilewski still fails to cure the defect of Tsuria and En-Seung as discussed above, and as such, claims 6 and 18, which depend from claims 1 and 17, respectively, are patentably distinguishable over the suggested combination.

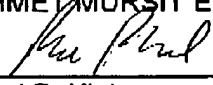### Rejection of claim 19 in view of Tsuria, En-Seung and Smyers

Applicants submit that even assuming arguendo that Smyers provides the teachings alleged by the examiner, Smyers fails to cure the defect of Tsuria and En-Seung as discussed above, and as such, claim 19, which depends from claim 17, is patentably distinguishable over the suggested combination.

Customer No. 24498
Attorney Docket No. RCA89462
Final Office Action Date: 3/16/2007

Conclusion

Having fully addressed the Examiner's rejections it is believed that, in view of the preceding amendments and remarks, this application stands in condition for allowance. Accordingly then, reconsideration and allowance are respectfully solicited. If, however, the Examiner is of the opinion that such action cannot be taken, the Examiner is invited to contact the applicants' attorney at (609) 734-6815, so that a mutually convenient date and time for a telephonic interview may be scheduled.

Respectfully submitted,
AHMET MURSIT ESKICIOGLU, ET AL.

By:

Paul P. Kiel
Attorney for Applicants
Registration No. 40,677
Phone No. 609-734-6815

THOMSON Licensing LLC
PO Box 5312
Princeton, NJ 08543-5312

Date: 3/22/10